

## PRIVACY IMPACT ASSESSMENT

Please submit your responses to your Liaison Privacy Official  
[http://intranet.epa.gov/privacy/pdf/lpo\\_roster.pdf](http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf).

If you need further assistance contact Marlyn Aguilar, at [aguilar.marlyn@epa.gov](mailto:aguilar.marlyn@epa.gov) or (202) 566-0012.

**System Name:** eDiscovery Enterprise Tool Suite, EPA-63

**Preparer:** Brian Thompson

**Office:** eDiscovery Division, Office of Enterprise Information Programs, Office of Environmental Information

**Date:** October 16, 2018

**Phone:** (202) 564-4256

**Reason for Submittal:** New PIA  Revised PIA  Annual Review  Rescindment

This system is in the following life cycle stage(s):

Definition

Development/Acquisition

Implementation

Operation & Maintenance

Rescindment/Decommissioned

**Note:** Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).

The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).

### Provide a general description/overview of the system:

The eDiscovery Enterprise Tool Suite is a combination of several electronic tools that together assist with the preservation, search, processing, review and production of electronically stored information (ESI) in support of legal discovery or to respond to other formal information requests, such as FOIA requests and congressional inquiries.

The information collected and maintained in the eDiscovery Enterprise is not new data, but copies of existing data that reside on EPA systems. The eDiscovery Enterprise Tool Suite does not specifically collect PII data elements; however, if PII is collected as part of a discovery matter, then the PII will be maintained in the system.

### Section 1.0 Authorities and Other Requirements

employees, contractors, and grantees who have been identified as potential information collectors in the system will also contain the names and EPA email addresses of EPA

information from custodians and may contain personally identifiable information. The wide-ranging and potentially include emails, documents and other sources of ESI

formal information request. Information collected and contained in the system can be designed search criteria that relate to a litigation, investigation, FOIA matter or other

EDiscovery Collection Files. The collection files contain all information responsive to

- EDiscovery Case Tracking Files. The case tracking files contain information about the (FOIA) matter or other formal information request.

cases created in response to a litigation, investigation, Freedom of Information Act provided EPA email addresses and who have been identified as custodians of information that needs to be preserved in the anticipation of litigation.

EDiscovery Litigation Hold Files. The litigation hold files contain the names and email addresses of EPA employees and EPA contractors, items, or grantees who have been

mainstays (e.g., data elements, including name, address, DOB, SSN).

- 2.1 Identify the information the system collects, uses, disseminates, or**
- The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

## Section 2.0 Characterization of the Information

There are no Office of Management and Budget (OMB) control numbers or information collections, as defined by the Paperwork Reduction Act, that will be used to collect information that will be maintained in the EDiscovery Enterprise Tool Suite.

collection. If there are multiple forms, include a list in an appendix.

(PRA), provide the OMB Control number and the agency number for the

If the information is covered by the Paperwork Reduction Act

Yes, a security plan for the system was completed.

**1.2 Has a system security plan been completed for the information system(s) supporting the system?**

The statutory authority for the EDiscovery Enterprise Tool Suite can be found in 44 U.S.C. § 3506, which establishes federal agencies' responsibilities for managing information resources and 40 U.S.C. § 11315, which establishes the responsibilities of the agency's Chief Information Officer to manage agency information resources.

**1.1 What specific legal authorities and/or agreements permit and**

define the collection of information by the system in question?

custodians. Privacy information may be included in the ESI collected and maintained in the system.

**2.2 What are the sources of the information and how is the information collected for the system?**

The sources of information are custodians' local workstations, network file servers, collaboration tools, electronic records repositories, email and loose electronic documents (e.g., MS Word, MS PowerPoint, PDF, etc.). The information is extracted from its native source using the eDiscovery Enterprise Tool Suite, which is operated by EPA's eDiscovery technical team. Collections are based on custodian, date range and search or filtering criteria (e.g. keywords) that relate to the matter.

**2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.**

The system does not use information from commercial sources, such as information obtained from data aggregators. The system does not collect publicly available data, meaning information received from the internet, news feeds or from state or local public records, such as court records. Any data that reside in the eDiscovery Enterprise Tool Suite have been collected from other EPA systems to determine the data's relevance to a particular matter, and the collected data may or may not include data that EPA has made or will make available to the public.

**2.4 Discuss how accuracy of the data is ensured.**

The data retained in the system are copies of information already residing on other EPA systems. Therefore, the accuracy of the data in the eDiscovery Enterprise Tool Suite depends on the accuracy of the data in the source systems. Data in the eDiscovery Enterprise Tool Suite are not collected from non-EPA systems. In addition, accuracy of the data residing in the eDiscovery Enterprise Tool Suite is maintained by controlling access to the records in the Tool Suite. Access is restricted to a limited number of authorized users with the appropriate security clearances and password permissions; access is further limited by user type.

**2.5 Privacy Impact Analysis: Related to Characterization of the Information**

**Privacy Risk:**

There is a risk that in the process to collect and determine whether information is relevant to a matter, more information is collected and maintained in the eDiscovery Enterprise Tool Suite than is relevant to the matter.

**Mitigation:**

<b>Section 3.0 Uses of the Information</b>	
<b>3.1</b>	<b>Describe how and why the system uses the information.</b>
<i>The following questions require a clear description of the system's use of information.</i>	
<b>3.2</b>	<b>How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>.</b>
	Data in the system will be retrieved by custodian name and/or email address.
<b>3.3</b>	<b>If the system retrieves information by personal identifier, what types/elements of information about the user are being retrieved?</b>
	Information collected using the eDiscovery Enterprise Tool Suite is based on custodian name and email address. The records collected by custodian name or email address may include emails, documents and other sources of ESL and may contain personally identifiable information.
<b>3.4</b>	<b>What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?</b>
	EPA-63, eDiscovery Enterprise Tool Suite.

**3.5 Does the system use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how EPA plans to use such results.**

The eDiscovery Enterprise Tool Suite does not conduct electronic searches, queries or analyses to make predictions about the future or identify anomalies. The information collected using the eDiscovery Enterprise Tool Suite is based on custodian, date range and search or filtering criteria (e.g., keywords) that relate to the matter.

**3.6 Privacy Impact Analysis: Related to the Uses of Information**

**Privacy Risk:**

There is a risk that the information maintained in the eDiscovery Enterprise Tool Suite is used for purposes other than the purpose for which it was collected or the information is accessed by unauthorized users.

**Mitigation:**

This risk is mitigated by restricting access to the system and providing training. The uses of the information for the eDiscovery Enterprise Tool Suite are relevant and necessary for legal discovery and to respond to FOIA requests, congressional inquiries and other formal requests for information. To ensure information is handled in accordance with the uses described above, a limited number of individuals can request the use of the system for a particular matter and they are asked to identify the purpose for the request (e.g., litigation, FOIA, congressional inquiry etc.). Additionally, there are role-based access control for users of the system. Users are provided access to information in the system based on their need to know. Individuals working on a particular matter will be given access only to the information related to that matter. The technical team and system administrators are given full access to information in the system to perform technical and administrative functions. The system is maintained in secure, access-controlled areas and buildings. Users of EPA systems are required to complete security and privacy training on an annual basis to ensure continued access to the system.

## **Section 4.0 Notice**

*The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.*

**4.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.**

An individual identified as a custodian of information in a litigation, FOIA, congressional or other matter may or may not be notified in advance of a collection of their electronically stored information (ESI).

## Section 5.0 Access and Data Retention by the System

This risk is mitigated through the SORN and PLA for the eDiscovery Enterprise Tool Suite and the SORNs and PLAs for the source systems of the information.

### Mitigation:

There is a risk that the individual may not be aware that information is being maintained in the eDiscovery Enterprise Tool Suite.

### Privacy Risk:

#### 4.3 Privacy Impact Analysis: Related to Notice

There are no opportunities for individuals to consent to uses, decline to provide information or opt out of the collection or sharing of the information.

#### 4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

A SORN for the eDiscovery Enterprise Tool Suite will be published in the Federal Register to provide written notice of the Agency's intent to collect information from individuals for the purpose of legal discovery or responding to a FOIA request, congressional inquiry or other official request for information.

"In proceeding and accessing U.S. Government information and information systems, you acknowledge that you fully understand and consent to all of the following:...4) you have no reasonable expectation of privacy regarding any communication used, transmitted, or stored on U.S. Government communication systems or information used or stored on U.S. Government information systems; 5) at any time, the U.S. Government may for any lawful government purpose, search and seize any unauthorized or unauthorized device, to include non-U.S. Government owned devices, that stores U.S. Government information; 6) any communications or information used, transmitted, or stored on U.S. Government information systems or devices, that stores U.S. Government information; 7) any communications or information used, transmitted, or stored on U.S. Government information systems;..."

However, when a user of an EPA computer logs onto his/her computer, he/she is provided with a government warning notice which states,

*The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.*

**5.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?**

Access to the eDiscovery Enterprise Tool Suite is restricted to a limited number of authorized users with the appropriate security clearances and password permissions. Access to the system is further limited by user type. System administrators have full access to the tool suite, including the ability to perform administrative functions. Other users have limited access particularized to the specific functions they need to perform in the Tool Suite rather than the whole lot of data. Authorized users include federal and contract staff located throughout the country. The system is maintained in secure areas and buildings with physical access controls.

**5.2 Are there other components with assigned roles and responsibilities within the system?**

Authorized users of the eDiscovery Enterprise Tool Suite include federal and contract staff located throughout the country in EPA's Program Offices and Regions. This includes eDiscovery technicians, case managers and other federal and contract staff supporting the Discovery Services Program in OEI and other EPA Program Offices and Regions.

Employees reviewing collected data to determine the data's relevance to a particular matter will have access to the information maintained in the eDiscovery Enterprise Tool Suite, as appropriate. These employees may be assigned to the various EPA's Program Offices and Regions.

**5.3 Who (*internal and external parties*) will have access to the data/information in the system? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?**

Authorized users of the eDiscovery Enterprise Tool Suite include federal and contract staff located throughout the country. This includes eDiscovery technicians, case managers and other federal and contract staff supporting the Discovery Services Program. Employees reviewing collected data to determine its relevance to a particular matter will have access to the information maintained in the eDiscovery Enterprise Tool Suite, as appropriate.

FAR clauses 52.224-1 and 52.224-2 have been included in the contract for support of the Discovery Services Program and will be included in future contracts.

**6.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.**

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

## Section 6.0 Information Sharing

This risk is mitigated through the implementation of the CIO Procedure 2155-P-03, Collection and Retention Procedures for Electronically Stored Information (ESI) Collected Using E-Discovery Tools. Further, if a litigation hold is in place, the normal disposition of records is suspended and the Agency must preserve this information until the hold is lifted.

### Mitigation:

There is a risk that the eDiscovery Enterprise Tool Suite may retain data longer than the sources systems' retention periods.

### Privacy Risk:

#### 5.7 Privacy Impact Analysis: Related to Retention

Yes

**5.6 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?**

RCS 1012: RCS 0089

Explains how long and for what reason the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Designated users only can request the use of the eDiscovery Enterprise Tool Suite. These specific matters is given to users who are part of the team working on the particular matter. Users are identified by the Information Management Official for that organization. Access to

**5.4 What procedures are in place to determine which users may access the information and how does the system determine who has access?**

Information produced from the eDiscovery Enterprise Tool Suite may be shared with external parties, as appropriate. In discovery matters, information may be shared with the Department of Justice or opposing counsel, as appropriate. For FOIA matters, information will be provided to the FOIA requester and subject to the nine FOIA exemptions for disclosure under the FOIA. Information from the system will be shared with a member of Congress or congressional staff in response to a congressional inquiry. Such disclosures are covered under EPA's General Routine Uses for records maintained in an EPA system of records and, therefore, memoranda of understanding or interagency agreements have not been issued for these purposes. EPA's General Routine Uses are published here: <https://www.federalregister.gov/documents/2008/01/14/E8-445/amendment-to-general-routine-uses#h-14>.

**6.2 Describe how the external sharing noted in 6.1 is compatible with the original purposes of collection in the SORN noted in 3.4.**

The Agency will publish a SORN for the eDiscovery Enterprise Tool Suite indicating that EPA's General Routine Uses A, C, D, E, F, G, H, I, K, and L apply to this system. Refer to <https://www.federalregister.gov/documents/2008/01/14/E8-445/amendment-to-general-routine-uses> for a full explanation of these routine uses.

**6.3 Does the agreement place limitations on re-dissemination?**

Disclosures of information residing in the eDiscovery Enterprise Tool Suite are covered under EPA's General Routine Uses for records maintained in an EPA system of records and, therefore, memoranda of understanding or interagency agreements have not been issued for these purposes.

**6.4 Describe how the system maintains a record of any disclosures outside of the Agency.**

The eDiscovery Enterprise Tool Suite uses the existing processes and procedures at EPA for recording disclosures of information as appropriate to the situation (e.g., FOIAonline for FOIA requests, the correspondence management system (CMS) for congressional requests, and chain of custody forms for disclosures to DOJ), and it does not establish or maintain an additional record of the disclosures within the system.

**6.5 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?**

Disclosures of information residing in the eDiscovery Enterprise Tool Suite are covered under EPA's General Routine Uses for records maintained in an EPA system of records and, therefore, memoranda of understanding or interagency agreements have not been issued for these purposes.

<https://www.ecfr.gov/cgi-bin/text-idx?SID=e744de790bcd49ed29e09e5d4efee&mc=true&node=pt40.1.16&rgn=div5>.

The procedures for identifying the records to be changed and the corrective action sought are described in EPA's Privacy Act regulations at 40 CFR part 16.

## 7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

<https://www.ecfr.gov/cgi-bin/text-idx?SID=e744de790bcd49ed29e09e5d4efee&mc=true&node=pt40.1.16&rgn=div5>. Any other requests for access must be made in accordance with the procedures described in EPA's Privacy Act regulations at 40 CFR part 16 (<https://www.ecfr.gov/cgi-bin/text-idx?SID=e744de790bcd49ed29e09e5d4efee&mc=true&node=pt40.1.16&rgn=div5>).

U.S.C. § 552(k)(2). Additionally, EPA is using the EDiscovey Enterprise Tool Suite for civil and criminal cases and investigations, therefore the information in the system is exempt from certain affirmative access and amendment provisions. The Agency's National Privacy Program will publish a regulatory action to revise the Agency's Privacy Act implementation regulations, along with the SORN for the EDiscovey Enterprise Tool Suite, to exempt the system from certain provisions of the Privacy Act pursuant to § U.S.C. § 552(j)(2) and § 552(k)(2).

Because the information in the EDiscovey Enterprise Tool Suite consists of data provided by other source systems, information responsive to access requests will most likely be obtained from the source system of records.

## 7.1 What are the procedures that allow individuals to access their information?

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

This risk is mitigated by restricting access to the system to authorized users, and further restricting access to user groups based on their particular functions. Information will be shared for the stated purposes.

### Mitigation:

There is a risk that a disclosure of information occurs in a manner not consistent with EPA's General Routine Uses.

### Privacy Risk:

## 6.6 Privacy Impact Analysis: Related to Information Sharing

**7.3 How does the system notify individuals about the procedures for correcting their information?**

The SORN for the system includes a section on procedures for contesting records, which are described in EPA's Privacy Act regulations at 40 CFR part 16 (<https://www.ecfr.gov/cgi-bin/text-idx?SID=e744de790bcd49ed29ef09e5d4e4fee&mc=true&node=pt40.1.16&rgn=div5>).

**7.4 Privacy Impact Analysis: Related to Redress**

**Privacy Risk:**

There is a risk that information believed to be inaccurate or erroneous cannot be corrected in the system, rather the information should be corrected in the source system.

**Mitigation:**

This risk is mitigated through the notice provided in the SORN for the source systems of information and the procedures for seeking corrective action described in EPA's Privacy Act regulations at 40 CFR part 16 (<https://www.ecfr.gov/cgi-bin/text-idx?SID=e744de790bcd49ed29ef09e5d4e4fee&mc=true&node=pt40.1.16&rgn=div5>).

## **Section 8.0 Auditing and Accountability**

*The following questions are intended to describe technical and policy based safeguards and security measures.*

**8.1 How does the system ensure that the information is used in accordance with stated practices in this PIA?**

The eDiscovery Enterprise Tool Suite is used to preserve, collect and review information from source systems and maintain this information for the purpose of legal discovery or responding to FOIA requests, congressional inquiries or other official requests for information. The ability to request the use of the eDiscovery Enterprise Tool Suite is limited to authorized requestors who are required to identify the purpose for their request to use of the system. Additionally, access to the records in the system is restricted to a limited number of authorized users with the appropriate security clearances and password permissions.

**8.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.**

The Agency's mandatory IT security training contains information on the proper handling of PII data.

## 8.3 Privacy Impact Analysis: Related to Auditing and Accountability

This risk is mitigated through annual security assessments that are conducted to ensure compliance with privacy requirements.

### Mitigation:

There is a risk that the required information privacy controls may not be implemented fully or correctly.

### Privacy Risks:

#### 8.3.1 Privacy Impact Analysis: Related to Auditing and Accountability